瑞星 **Lotus Domino** 邮件病毒监控系统使用手册

北京瑞星科技股份有限公司

目　录

瑞星 Lotus Domino 邮件病毒监控系统......1
1　安装......3
1.1　安装步骤......3
1.1.1　关闭 Lotus Domino 服务器和 Lotus Notes......3
1.1.2　安装瑞星 Lotus Domino 邮件监控程序......3
1.1.3　重新启动 Lotus Domino 服务器......7
1.1.4　加载瑞星设置图标......7
1.2　卸载步骤......10
2　立即扫描......11
2.1　设置......11
2.1.1　发现病毒的处理方法......11
2.1.2 件类型......12
2.1.3 查杀选项......12
2.1.4 其他选项......12
2.2 使用......13
3　实时监控......15
3.1　设置......15
3.1.1　发现病毒的处理方法......15
3.1.2 扫描文件类型......16
3.1.3 查杀选项......16
3.1.4 其他选项......16
3.2 使用......17
4 升级......18
4.1 设置......18
4.1.1 升级设置......18
4.1.2 网络设置......19
4.2 应用......19
5 日志......21

1 安装

1.1 安装步骤

1.1.1 关闭 Lotus Domino 服务器和 Lotus Notes

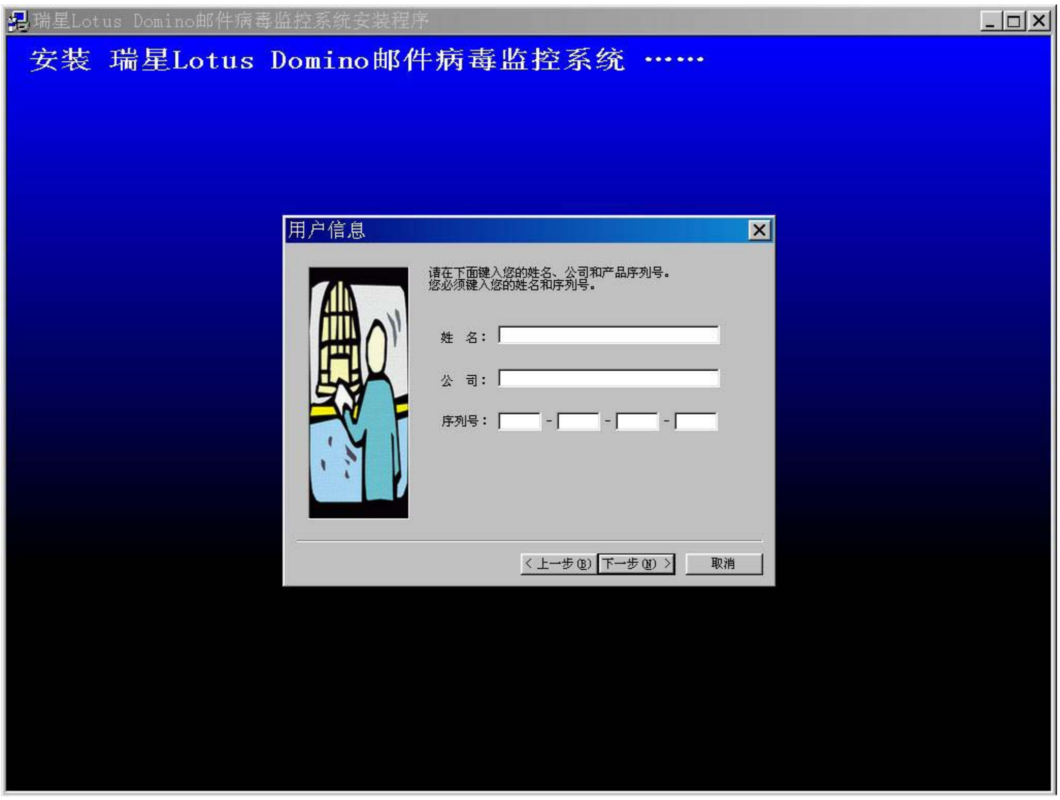
安装瑞星 Lotus Domino 邮件监控程序之前，请首先关闭 Lotus Domino 服务器和 Lotus Notes。

1.1.2 安装瑞星 Lotus Domino 邮件监控程序

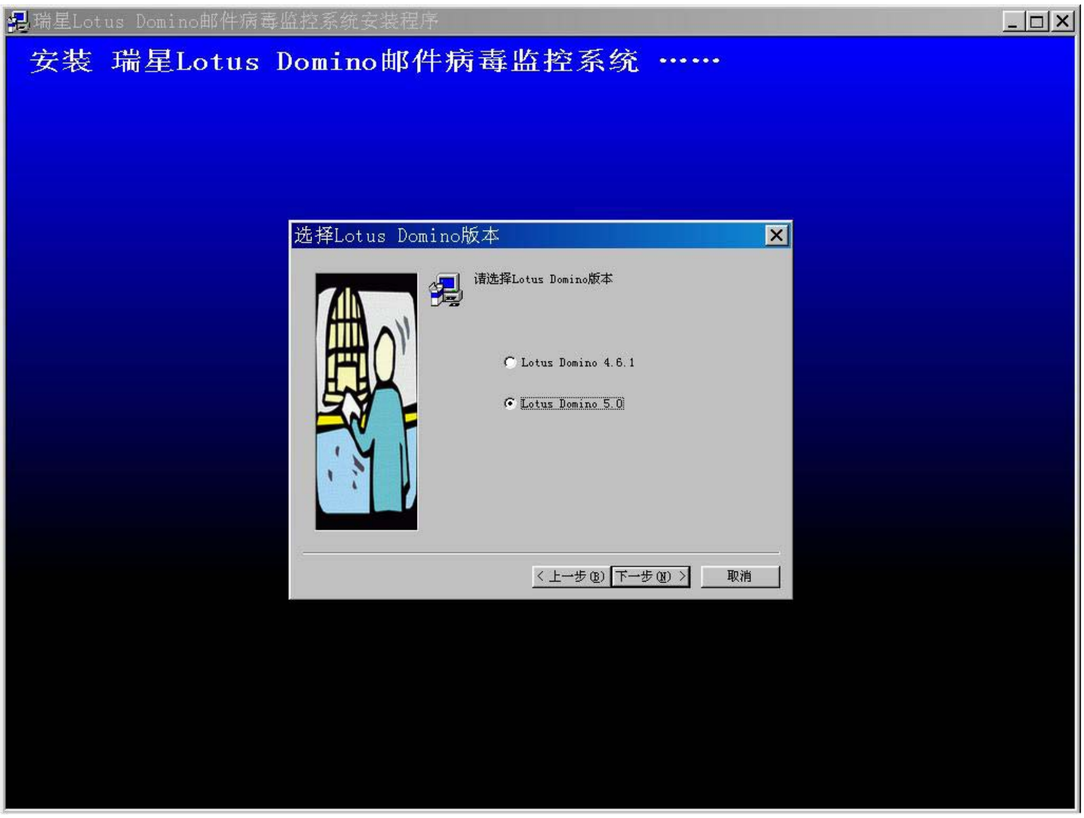
将安装光盘插入驱动器，执行瑞星 Lotus Domino 邮件监控程序安装程序：

单击“下一步>”进入下一步：

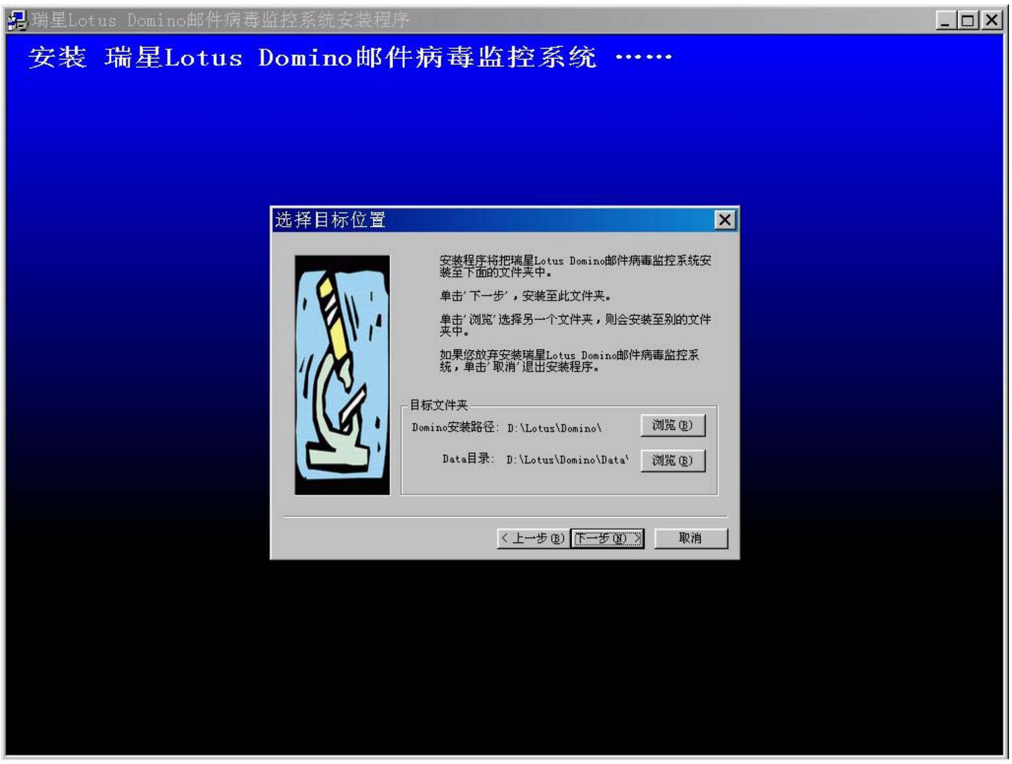
阅读安装许可协议后，如果不同意协议内容，选择“我不接受”，退出安装程序；如果同意许可协议内容，选择“我接受”，单击“下一步>”进入下一步：



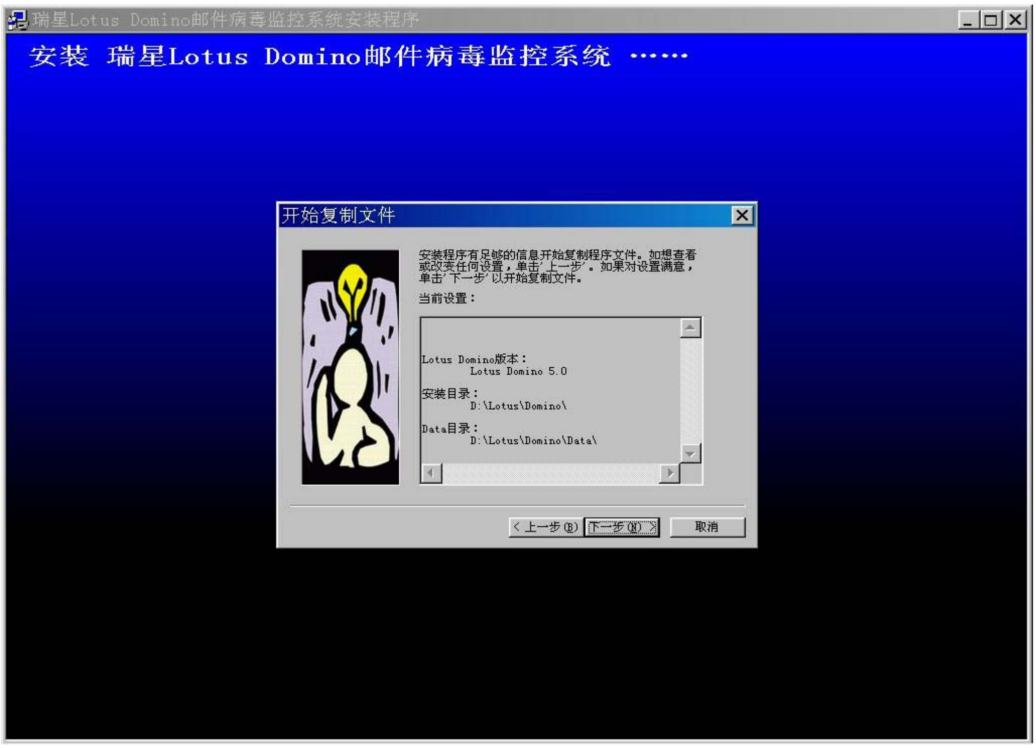
输入您的姓名、公司和序列号，其中姓名和序列号是必须的。单击“下一步>”进入下一步：



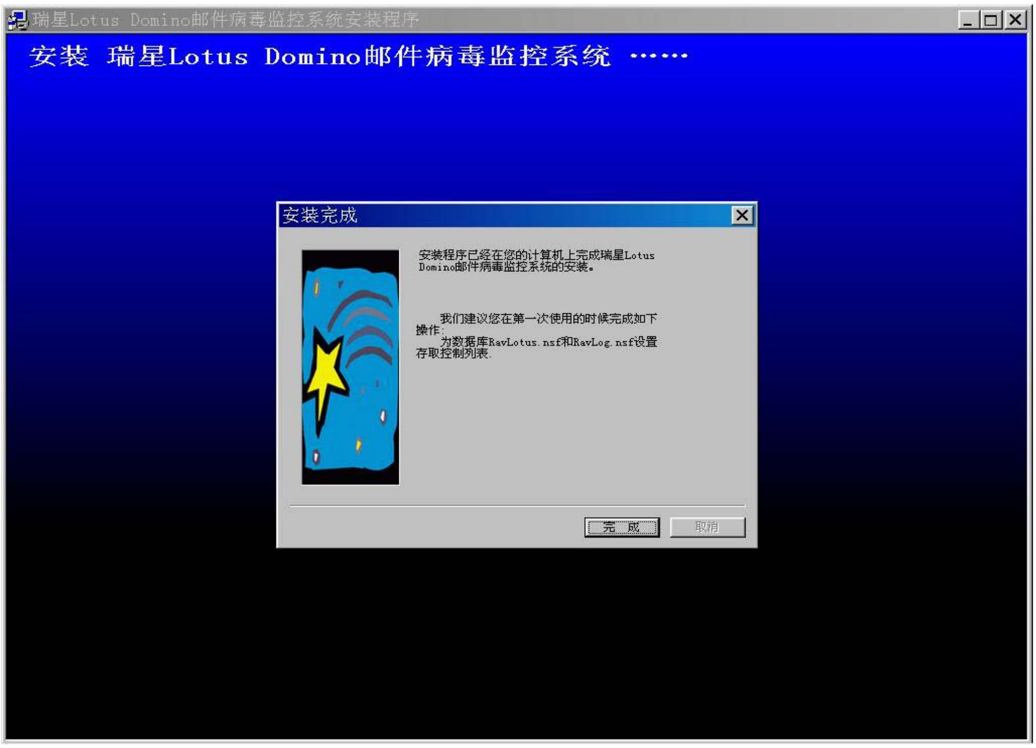
选择您使用的 Domino 服务器版本。注意，请务必正确选择，否则瑞星 Lotus Domino 邮件监控程序将不能正常工作。选择完毕，单击“下一步>”进入下一步：



选择瑞星Lotus Domino邮件监控程序的安装路径，这个路径必须和您计算机上Lotus Domino的安装路径相同,否则系统将不能正常运行。Domino安装目录是：Lotus Domino的安装路径；Data目录是：Lotus Domino的Data文件的安装目录。如果您的安装路径和显示的路径不同，请通过"浏览"按钮选择正确的安装目录。单击"下一步>"进入下一步：



在这一步，请确认安装信息正确，如果不正确，单击"<上一步"返回以前各步骤。如果一切正确，单击"下一步>"进入下一步。



看到以上画面，表示一切正常，瑞星 Lotus Domino 邮件监控程序安装完成。

注意：安装程序最后提示需要用户在第一次运行时最好设置 RavLotus.nsf 和 RavLog.nsf 数据库的存取列表，以保证邮件监控系统数据库的设置只能由系统管理员，以及管理员指定的用户来制定。RavLotus.nsf 存储系统的配置信息，RavLog.nsf 存储系统的日志信息。这两个数据库在 Lotus Domino 的 Data 目录下。

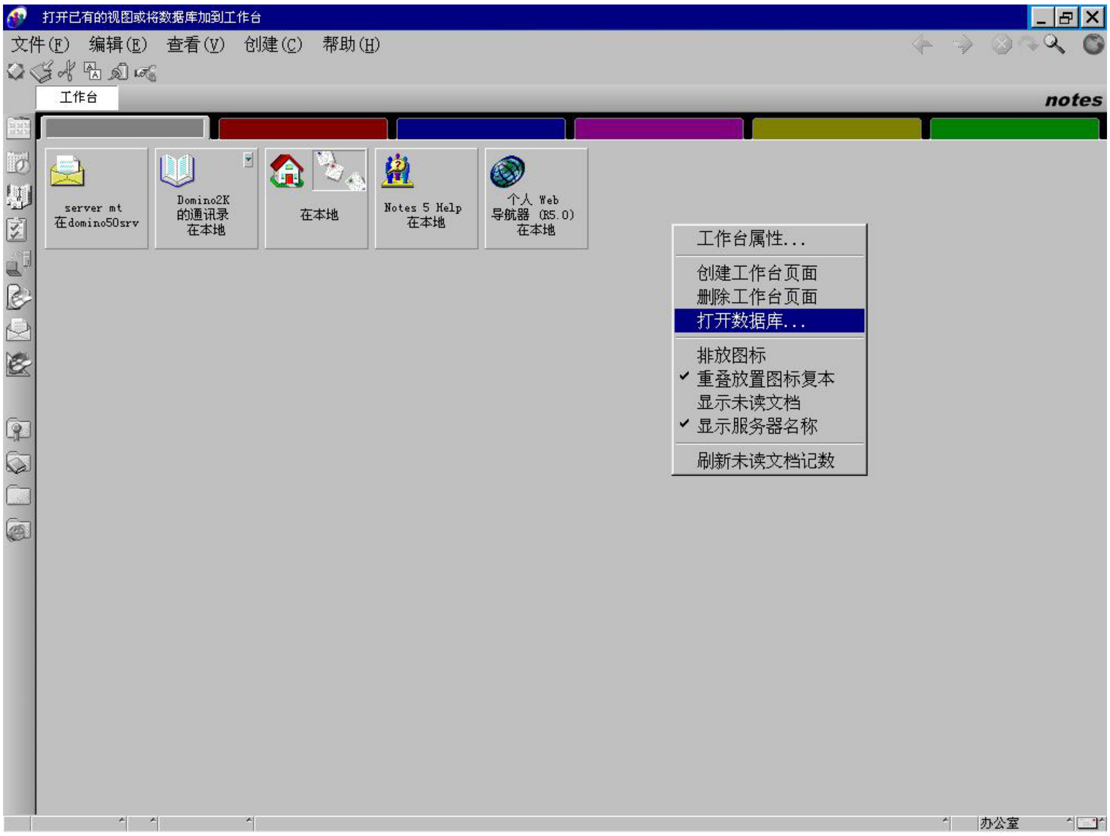
安装完毕后，在开始菜单->程序组中将新增一项“瑞星 Domino 邮件监控”。

1.1.3 重新启动 Lotus Domino 服务器

安装完毕，请重新启动 Lotus Domino 服务器。在 Lotus Domino 服务器的命令窗口，将看到瑞星 Lotus Domino 邮件监控程序的提示信息，表示安装成功，瑞星 Lotus Domino 邮件监控程序已经开始运行。

1.1.4 加载瑞星设置图标

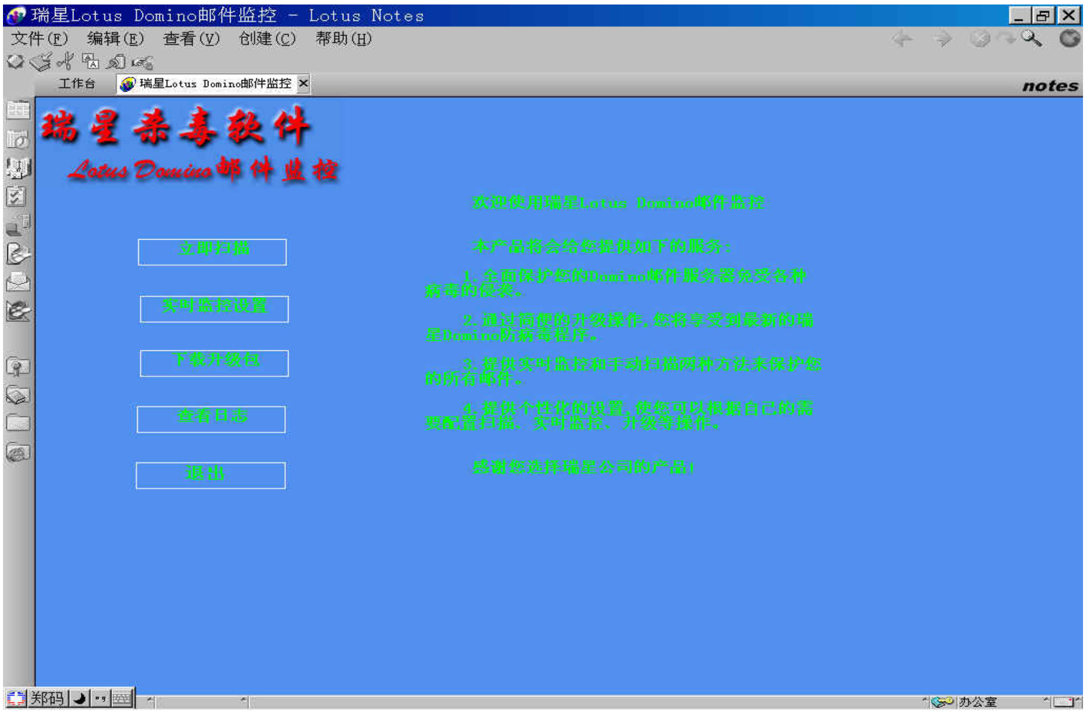
Lotus Domino 服务器启动后，打开 Lotus Notes 登陆到服务器，在 Lotus Notes 工作台的“文件”菜单中，选择“数据库”“打开”，或者在控制台界面上单击鼠标右键，



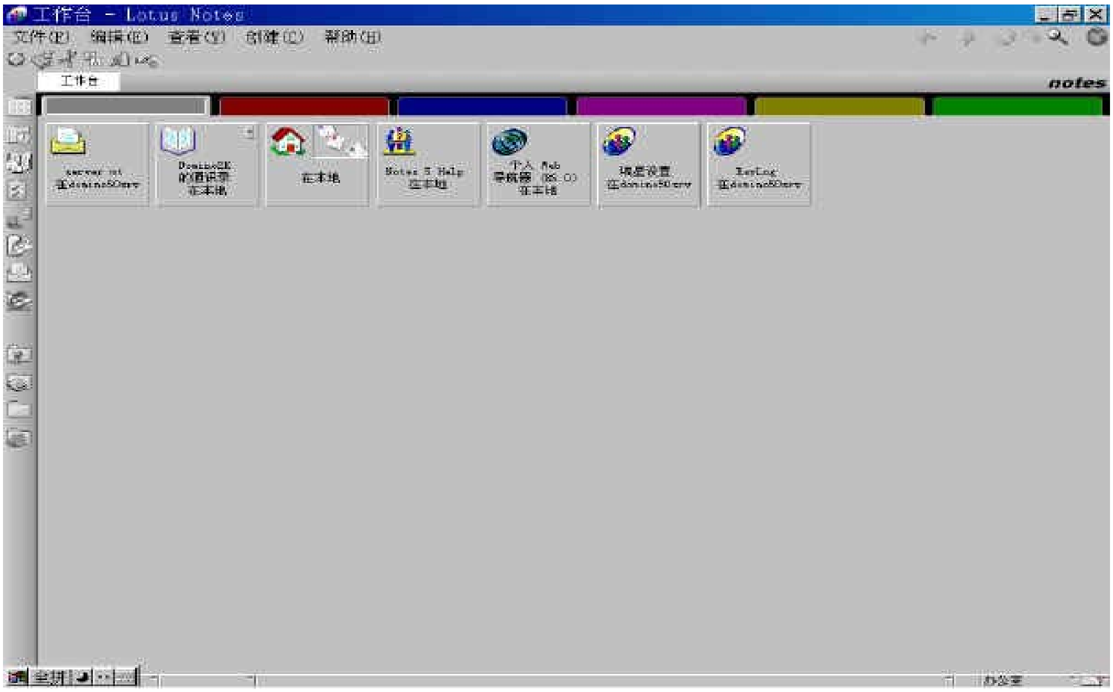
选择打开“打开数据库”，单击服务器的下拉箭头，选择 Domino 服务器：

然后在数据库列表栏里选择“瑞星设置”，

然后单击“打开”，弹出瑞星设置界面，



Lotus Notes 会在控制台上建立“瑞星设置”图标。



注意：添加瑞星设置图标后，需要用户自己设置 RavLotus.nsf 和 RavLog.nsf 数据库的存取列表。

设置存取控制列表：

1、在 Notes 工作台上右键单击瑞星设置数据库，然后从弹出的环境菜单中选择"存取控制"。

2、将您自己，或者指定的管理瑞星Lotus Domino邮件监控程序的用户，作为具有"删除文档"权限的"管理者"添加到存取控制列表中。

3、将默认存取级别更改为"不能存取者"。

对其它瑞星数据库（瑞星日志 RavLog.nsf）重复上述步骤。

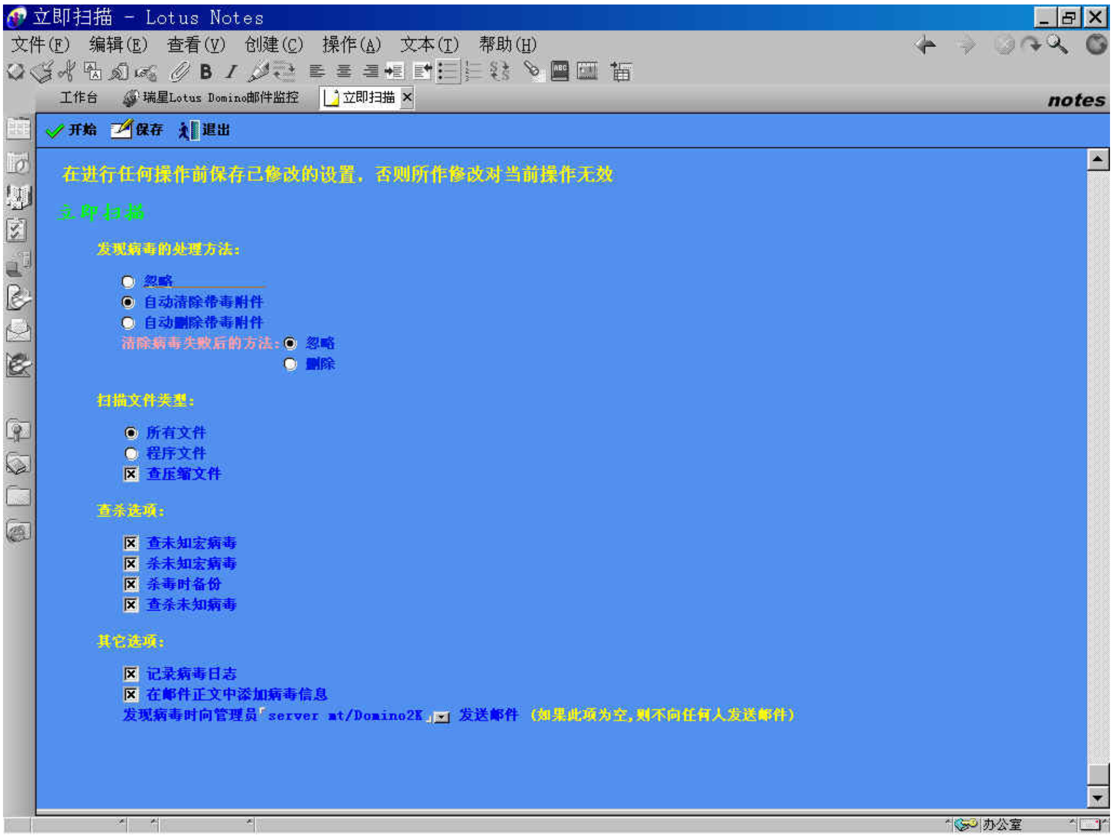
1.2 卸载步骤

从开始菜单->程序组中->瑞星 Domino 邮件监控中单击"卸载 Dominio 邮件监控"，瑞星 Lotus Domino 邮件监控程序将自动卸载。

2 立即扫描

“立即扫描”是一种可以在任何时刻运行的，监测病毒的扫描。扫描 Data 目录中的“所有数据库”。

从 Notes 控制台上双击瑞星设置，进入瑞星 Lotus Domino 邮件监控系统，单击立即扫描，进入立即扫描界面：



2.1 设置

立即扫描的配置内容分为发现病毒的处理方法、扫描文件类型、查杀选项和其他选项四项。

2.1.1 发现病毒的处理方法

功能：在实时监控和扫描病毒的过程中，如果发现病毒后，系统所采取的警告信息方式。

各选项功能如下：
忽略：不对病毒做任何处理，但把病毒信息记录在警告信息里。
自动清除：直接清除附件文件里的病毒，并把病毒信息记录在警告信息里。
自动删除：直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

其中，清楚病毒失败后的处理方法，此项设置主要针对一些病毒不能被清除的带病毒文件。例如，一个携带病毒的文件，现在版本不能直接清除或删除文件里的病毒文件，软件在处理这些文件时就是清除失败，那么软件处理此类性文件时即按照此项设置处理。
忽略：清楚病毒失败后，不对病毒做任何处理，但把病毒信息记录在警告信息里。
删除：清楚病毒失败后，直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

注意：所有的经过杀毒处理的文件，都在病毒隔离区有备份，用瑞星病毒隔离系统可以看到，前提是在查杀选项里选择了“杀毒时备份”。

2.1.2 件类型

功能：设置实时监控和手动扫描时的文件类型。可以选择查杀所有文件或者只查杀程序文件，查杀同时可以复选是否查杀压缩文件。
程序文件指 EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、DOC、DOT、XLS、XLT 等扩展名的文件。

2.1.3 查杀选项

查未知宏病毒：选择后可检测出携带未知宏病毒的文件和带有宏的 Office 文件。
杀未知宏病毒：把携带未知宏病毒的文档重的宏去掉。
杀毒时备份：当您在查杀选项中选择了“杀毒时备份”，那么所有您清除或删除的染毒文件都会在“病毒隔离系统”中隔离起来，并可安全的恢复，避免设置或误操作造成的文件丢失损坏。
查杀未知病毒：指查杀文件中可能含有的未知病毒

2.1.4 其他选项

记录病毒日志：把在扫描时的病毒检测结果记录在日志里。
在邮件正文中添加病毒信息：在邮件的正文里添加病毒检测结果。
发现病毒时向管理员发送邮件：选择一个用户，当扫描发现病毒的时候就向此用户发送一封警告邮件。如下图：

注意：在进行任何操作前，包括扫描、退出，请保存以修改的设置，否则，所作的修改对当前操作无效。

2.2 使用

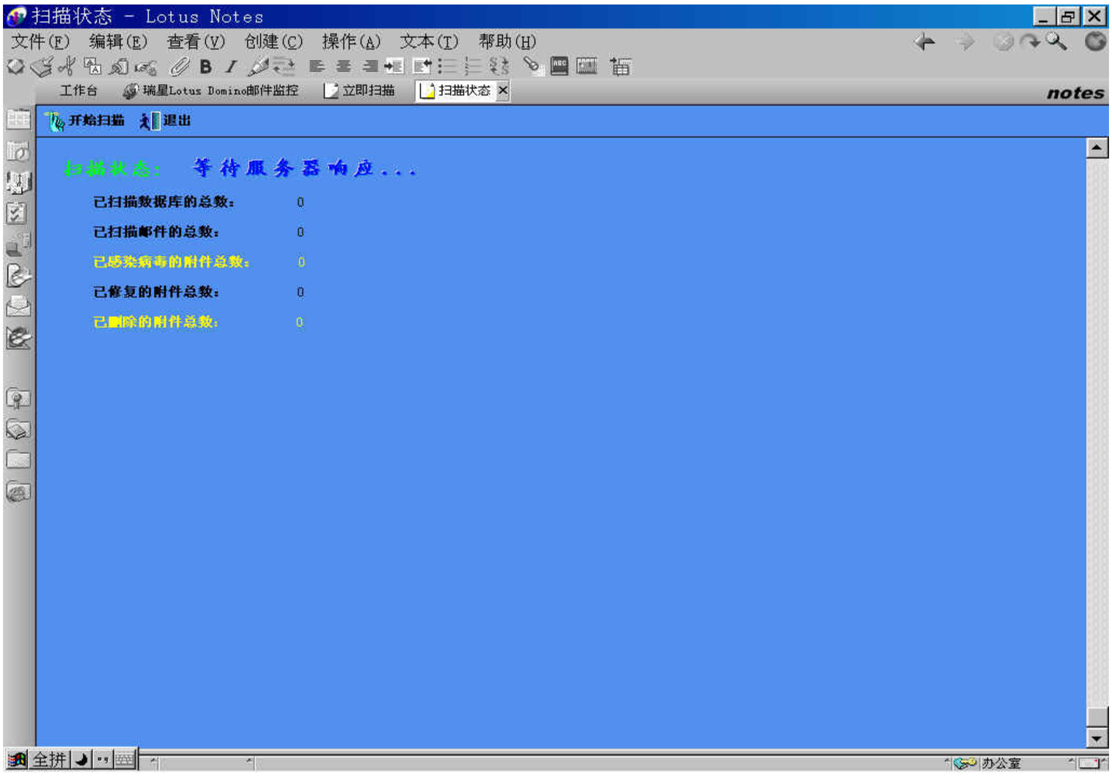
要开始立即扫描，请执行以下步骤：

1、从瑞星杀毒的主窗口，单击“立即扫描”

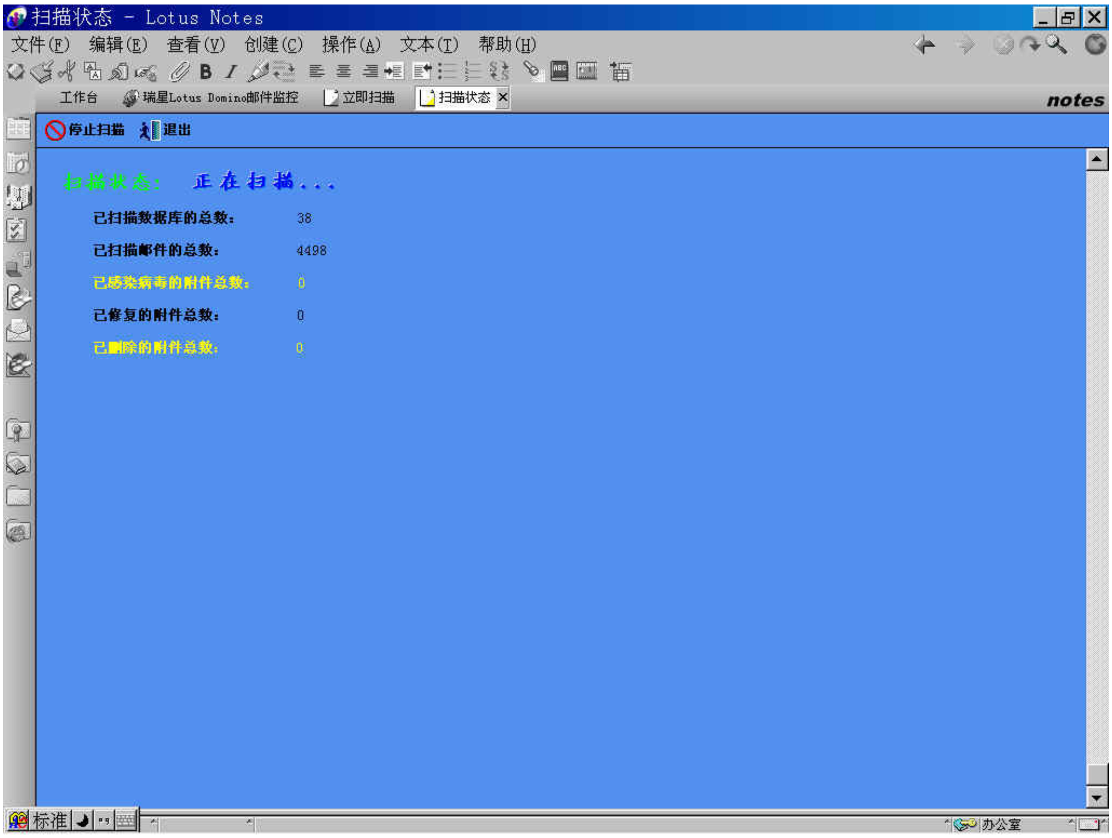
2、修改立即扫描设置选项，修改完成后请单击“保存”按钮保存设置

3、在该表单顶部的“操作栏”上，单击“开始”按钮

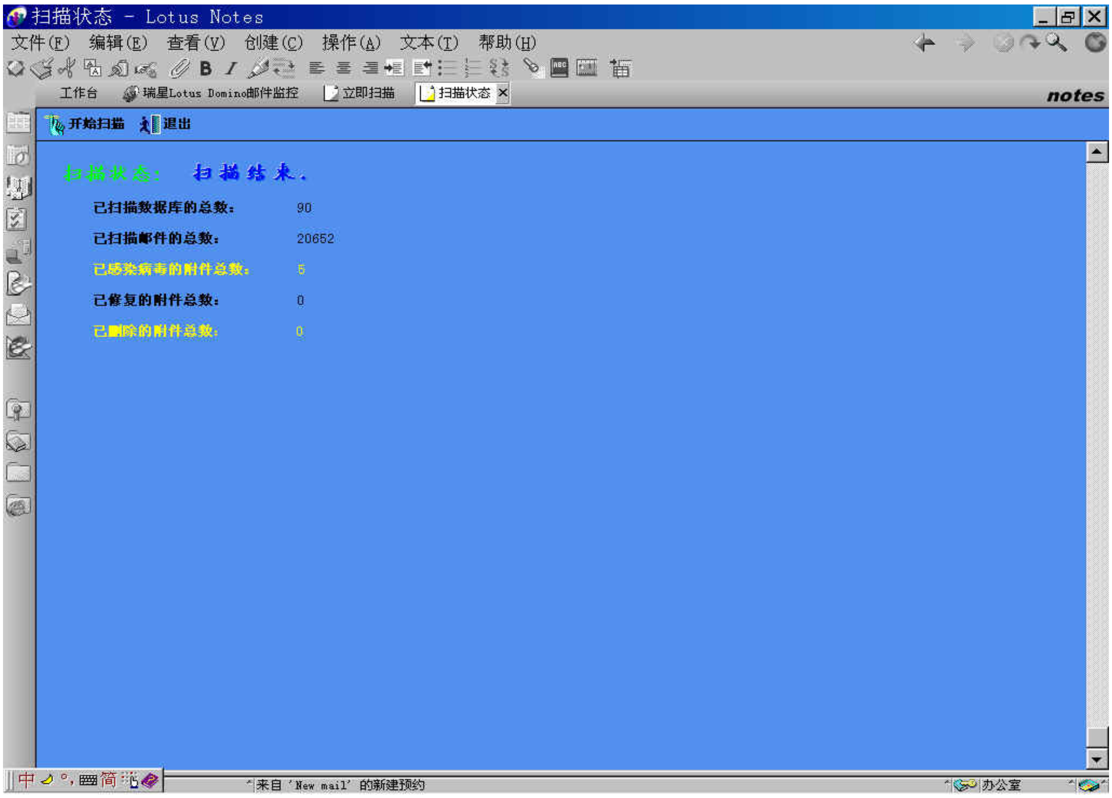
该扫描立即开始运行。首先，程序等待服务器响应，如下图：



当服务器开始响应的时候，开始扫描数据库，显示



扫描完成后，扫描状态显示扫描完成，并且显示具体病毒检测结果，



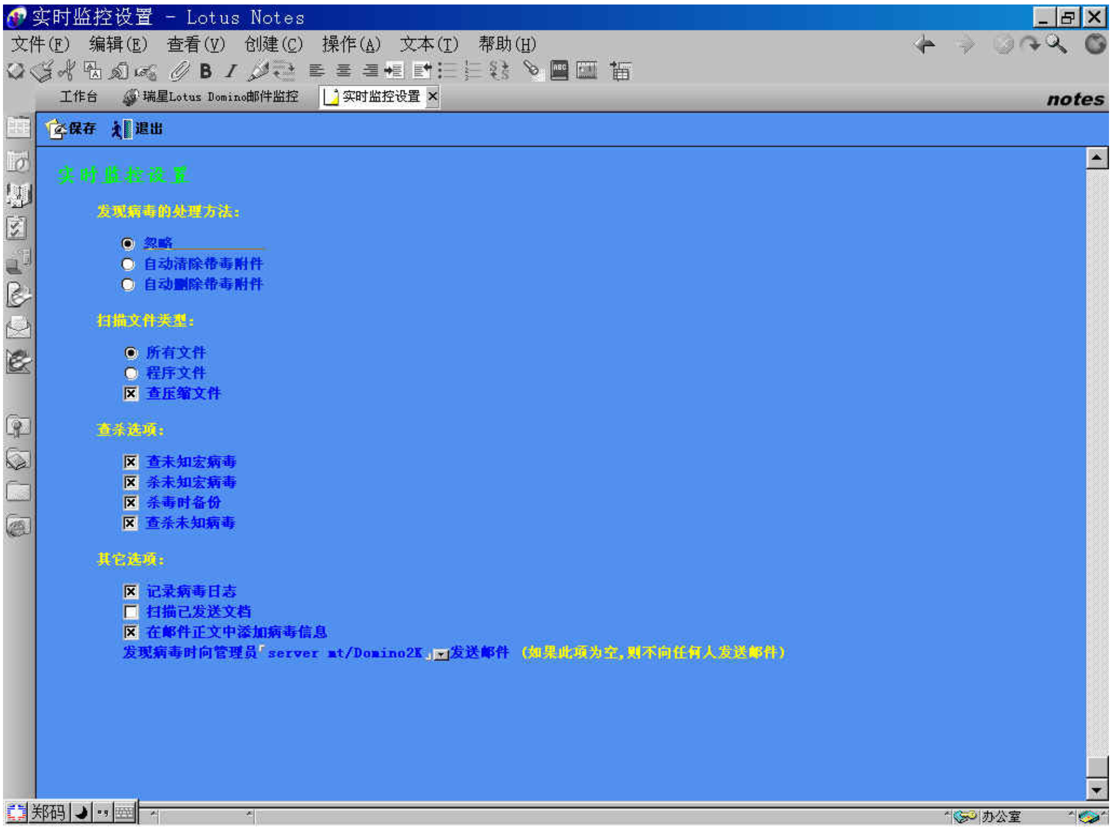
自此，扫描操作过程结束。

3 实时监控

实时监控，是一种实时的对写入数据库的文档的扫描。

3.1 设置

立即扫描的配置内容分为发现病毒的处理方法、扫描文件类型、查杀选项和其他选项四项。从 Notes 控制台上双击瑞星设置，进入瑞星 Lotus Domino 邮件监控系统，单击实时监控设置，进入实时监控设置界面：



3.1.1 发现病毒的处理方法

功能：在实时监控和扫描病毒的过程中，如果发现病毒后，系统所采取的警告信息方式。

各选项功能如下：
忽略：不对病毒做任何处理，但把病毒信息记录在警告信息里。
自动清除：直接清除附件文件里的病毒，并把病毒信息记录在警告信息里。
自动删除：直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

其中，清楚病毒失败后的处理方法，此项设置主要针对一些病毒不能被清除的带病毒文件。

例如，一个携带病毒的文件，现在版本不能直接清除或删除文件里的病毒文件，软件在处理这些文件时就是清除失败，那么软件处理此类性文件时即按照此项设置处理。
忽略：清楚病毒失败后，不对病毒做任何处理，但把病毒信息记录在警告信息里。
删除：清楚病毒失败后，直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

注意：所有的经过杀毒处理的文件，都在病毒隔离区有备份，用瑞星病毒隔离系统可以看到，前提是在查杀选项里选择了“杀毒时备份”。

3.1.2 扫描文件类型

功能：设置实时监控和手动扫描时的文件类型。可以选择查杀所有文件或者只查杀程序文件，查杀同时可以复选是否查杀压缩文件。
程序文件指 EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、DOC、DOT、XLS、XLT 等扩展名的文件。

3.1.3 查杀选项

查未知宏病毒：选择后可检测出携带未知宏病毒的文件和带有宏的 Office 文件。
杀未知宏病毒：把携带未知宏病毒的文档重的宏去掉。
杀毒时备份：当您在查杀选项中选择了“杀毒时备份”，那么所有您清除或删除的染毒文件都会在“病毒隔离系统”中隔离起来，并可安全的恢复，避免设置或误操作造成的文件丢失损坏。
查杀未知病毒：指查杀文件中可能含有的未知病毒

3.1.4 其他选项

记录病毒日志：把在扫描时的病毒检测结果记录在日志里。
在邮件正文中添加病毒信息：在邮件的正文里添加病毒检测结果。
扫描已发送文档：

发现病毒时向管理员发送邮件：选择一个用户，当监控发现病毒的时候就向此用户发送一封警告邮件。如下图：

注意：在修改设置后，请保存所修改的设置，否则，所作的修改对实时监控无效。

3.2 使用

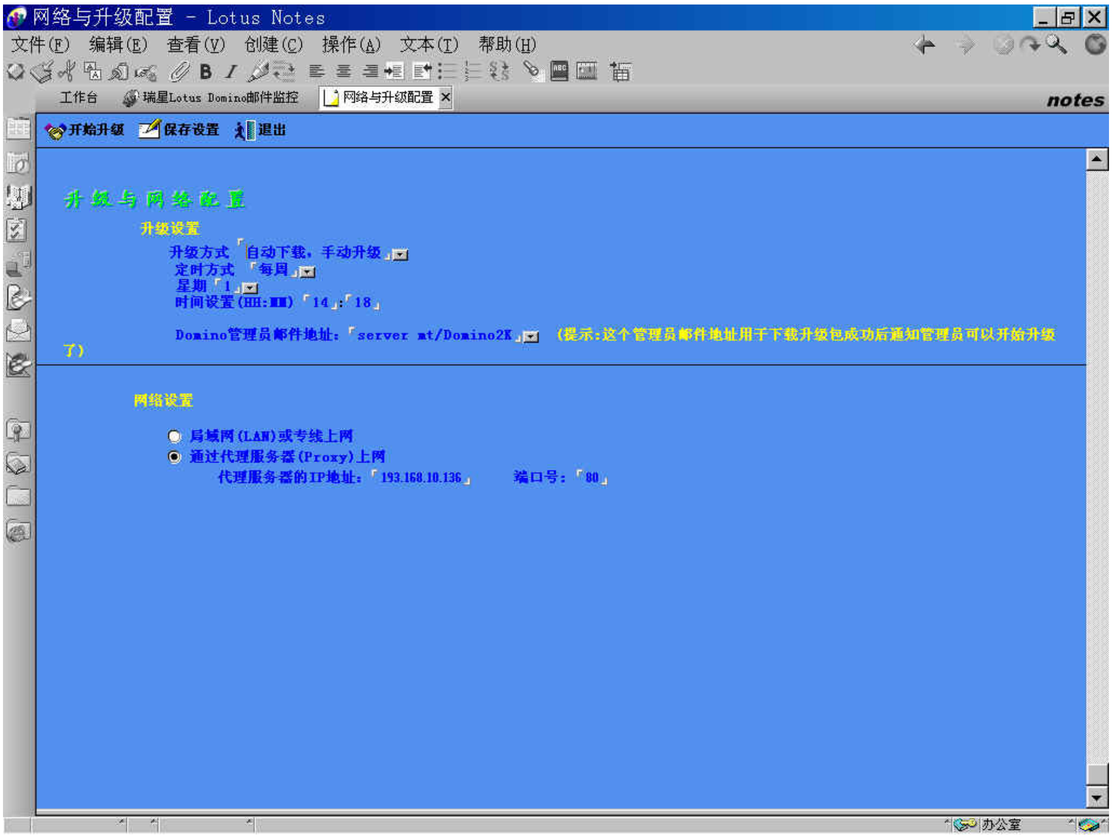
配置完实时监控设置后，实时监控就已经在运行了，只要向数据库写入并发送一个文档的时候，实时监控就会实时的扫描此文档。

4 升级

定期更新程序

4.1 设置

升级的设置可以分为两部分：升级设置和网络设置。



4.1.1 升级设置

升级设置来设定在进行升级之前，必须选择的最适合、最简便的升级方式，瑞星公司提供了 2 种升级方式，单击升级方式的下拉按钮，弹出一个选择框如下：

自动下载手动升级：按照设置的时间，定时自动下载升级程序。
设置时间只要通过单击相应的下拉按钮选择相应项就可以完成设置。

不使用自动设置：没有定时升级，用户可以在适当时间下载升级程序。

4.1.2 网络设置

局域网（LAN）或专线上网：如果安装瑞星 Lotus Domino 邮件病毒监控系统的计算机使用直接连接 Internet 的方式上网的，就可以选择此项。

通过代理服务器（Proxy）上网：如果安装瑞星 Lotus Domino 邮件病毒监控系统的计算机是通过代理服务器上网，就可以选择该项，网络设置会自动读取计算机上的 IE 使用的代理服务器的 IP 地址及端口号,用户也可以自己设置代理服务器的 IP 地址及端口号。

4.2 应用

系统升级方法可以分为自动下载手动升级和定时下载手工升级两种。

1. 自动下载手动升级
   1) 确定服务器已经可以连接 Internet。
   2) 从瑞星 Lotus Domino 邮件病毒监控系统单击下载升级包，到升级与网络设置界面
   3) 设置“网络设置”。
   4) 单击开始升级按钮，开始连接瑞星网站。
   5) 连上瑞星网站后，从网站上下载需要升级的程序，并给指定的管理员发出升级成功邮件。

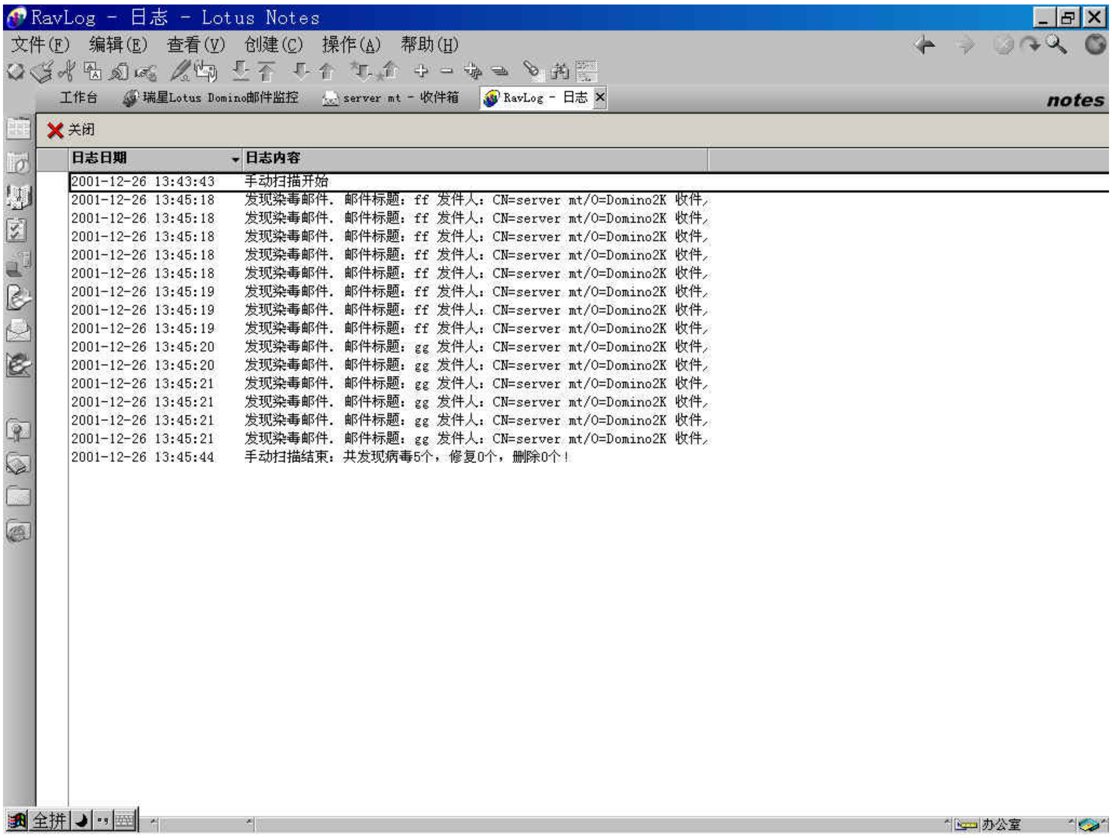
6) 关闭 Lotus Notes 和 Lotus Domino，运行升级程序即可完成升级。

2. 定时下载手动升级

1) 确定服务器已经可以连接 Internet。
2) 设置好网络设置。
3) 设置好定时下载的时间后，保存设置。
4) 升级程序会在指定时间开始连接瑞星网站下载升级程序。

5 日志

日志，纪录病毒检测信息。
阅读日志可以从 Lotus Notes 控制台单击瑞星日志，或者在瑞星 Lotus Domino 邮件监控系统的界面里单击查看日志，打开日志界面，查看具体的日志信息。



需要查看具体某一条信息时，直接用鼠标双击此条信息即可，具体信息内容如下：

事件时间：2001-12-26 13:45
事件内容：
　　发现染毒邮件. 邮件标题：ff　发件人：CN=server mt/O=Domino2K　收件人：CN=rising/O=Domino2K@Domino2K　染毒附件：1.rar>>HIDDEN.HTM　病毒名称：Script.trap.A　处理情况：忽略(邮件仍处于染毒状态)